CHAPTER 8

ELECTRONIC SECURITY SYSTEMS (ESS)

0800. PURPOSE. ESS are used to accomplish the following:

a. Permit more economical and efficient use of security personnel through the employment of mobile responding security forces instead of fixed guard posts and/or patrols.

b. Provide additional controls at critical areas or points.

c. Enhance the security force capability to detect and defeat intruders.

d. Provide the earliest practical warning to security forces of any attempted penetration of protected areas.

0801. ESS DETERMINATION FACTORS. The following factors must be considered to determine the feasibility and necessity of installing ESS equipment:

a. Mission.

b. Criticality.

c. Threat.

d. Geographic location of the installation or facility and location of facilities to be protected within each activity or installation.

e. Accessibility to intruders.

f. Availability of other forms of protection.

g. Life cycle cost of the system.

h. Construction of the building or facility.

i. Hours of operation.

j. Availability of a security force and expected response time to an alarm condition.

0802. INTRUSION DETECTION SYSTEM POLICY (IDS)

a. IDS are designed to detect, not prevent, actual or attempted penetrations. Therefore, IDS are useless unless supported by near-real-time assessment systems and prompt security force response when the systems are activated.

b. If a computerized IDS is used, it must be safeguarded against tamper.

c. Exterior or interior IDS will be standardized commercial equipment approved by CNO (N09N3). Presently installed IDS, not meeting the standards of this instruction, may continue to be used until replacement is necessary. Waivers/exceptions to use presently installed IDS are not required. Industry standards, including Underwriters Laboratory 611, 681, 1076, and 2050 should be met.

d. The data/signal transmission subsystem links sensors with control and monitoring consoles.

(1) Alarm transmission lines between the protected area and monitoring units will be protected by electronic line supervision systems to detect any signal cutting, shorting, tampering, splicing, or substitution on the sensor signal data transmission network, or by physical measures to prevent these actions.

(2) All sensors, transmitters, transponders, control units and other IDS components associated with a protected zone will be physically located within the protected area or, if not practical because of design or safety constraints, will alternatively be located within enclosures that are resistant to physical attack and are protected by sensors that will detect unauthorized opening or tamper.

e. Emergency Backup Power. IDS shall have an emergency power source to ensure the system's continuous operation. Emergency backup power sources usually consist of rechargeable batteries, emergency generator, or both.

f. Keyswitches, controllers, or other mechanisms used to activate and deactivate the IDS will be installed inside the protected area. Alarm activation delay devices are available which will allow sufficient time for personnel to exit the protected area after the system is activated.

g. IDS equipment whose housing can be opened will be fitted with anti-tamper devices which will initiate an alarm signal. The anti-tamper system will be in continuous operation regardless of the IDS mode of operation (access/secure/day/night).

h. Central Alarm Stations. Where practical, alarm consoles and central dispatching should be consolidated. These alarm stations should be in controlled access areas and properly protected. New construction should include ballistic protection. Consoles should not be visible to the exterior of the facility.

i. Alarm Response. The metric for response by the first law enforcement patrol is for priority A assets and life

threatening situations: 5 minutes. For all others: 15 - 45 minutes.

0803. MAINTENANCE

a. Requirements. Proper maintenance of an IDS is imperative.

b. IDS Functional Testing. Must be tested frequently enough to ensure system reliability.

(1) Consider recommendations of equipment manufacturers and installers.

(2) Consider actual experience.

(3) Comply with any more stringent criteria in other security directives when they apply.

(4) Keep records of when components are functionally tested. When components are found to be inoperable, records will indicate the date of discovery and the date the component was last positively verified to be working.

c. IDS Preventive Maintenance

(1) Commanding officers will:

(a) Establish an IDS preventive maintenance schedule based on industry standards and actual experience with the system.

(b) Keep records of their preventive maintenance and unscheduled component/system outages to include identification of component/system element which caused each outage, consequential costs, and manpower impact including compensatory measures.

0804. CLOSED CIRCUIT TELEVISION. Closed circuit television (CCTV) is very useful in physical security operations and is frequently used to complement an IDS or with Video Motion Detection. Closed circuit television may be used at entry points that are not manned continuously in conjunction with electronic access control systems. Closed circuit television also has application in the video detection and assessment of alarms. In this configuration, the CCTV can be triggered automatically or by personnel at the alarm control center and can be used to determine whether response forces should be dispatched. CCTV can minimize the number of security personnel normally needed for checking identification at gates, or for patrol or observation posts.

0805. ELECTRONIC ACCESS CONTROL SYSTEMS USING MAGNETIC STRIPES. All new acquisitions of electronic access control components involving use of magnetic stripes will adhere to specifications in reference (ac).